VIEW Certified Configuration Guide

Nortel

WLAN Security Switch 2300 Series with AP-2330

January 2008 Edition
1725-36082-001
Version F

Trademark Information

Patent Information

The accompanying product is protected by one or more US and foreign patents and/or pending patent applications held by Polycom, Inc.

Copyright Notice

Every effort has been made to ensure that the information in this document is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice and does not represent a commitment on the part of Polycom, Inc.

Notice

Polycom, Inc. has prepared this document for use by Polycom personnel and customers. The drawings and specifications contained herein are the property of Polycom and shall be neither reproduced in whole or in part without the prior written approval of Polycom, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Polycom reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Polycom to determine whether any such changes have been made.

No representation or other affirmation of fact contained in this document including but not limited to statements regarding capacity, response-time performance, suitability for use, or performance of products described herein shall be deemed to be a warranty by Polycom for any purpose, or give rise to any liability of Polycom whatsoever.

Contact Information

Please contact your Polycom Authorized Reseller for assistance.

Polycom, Inc.
4750 Willow Road,
Pleasanton, CA 94588
http://www.polycom.com

Introduction

Polycom's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between SpectraLink 8000 Wireless Telephones and wireless LAN (WLAN) infrastructure products. The products listed below have been thoroughly tested in Polycom's lab and have passed VIEW Certification. This document details how to configure the Nortel WLAN Security Switch 2300 Series and WLAN AP-2330/2330A/2330B with SpectraLink 8000 Wireless Telephones.

Certified Product Summary

Manufacturer:	Nortel: www.nortel.com		
Approved products:	WLAN Security Switches	Access points	
	2380 2361† 2360 2350	2330† 2330A 2330B	
Security:	WPA-PSK and WPA2-PSK		
2300 software version tested:	Release 5.0.11.4		
SpectraLink handset models tested:	e340/h340/i640	8020/8030	
SpectraLink handset software tested:	89.119	122.010 or greater	
SpectraLink radio mode:	802.11b	802.11b	802.11a
Maximum telephone calls per AP:	10	10	12 *
Recommended network topology:	Switched Ethernet (required)		

† Denotes products directly used in Certification testing.

* Maximum calls tested during VIEW Certification. The certified product may actually support a higher number of maximum calls for 802.11a radio modes.

Service Information

The access point (AP) must support SpectraLink Voice Priority (SVP). Contact your AP vendor if you need to upgrade the AP software.

Contacting Nortel Technical Support

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Additional information about the Nortel Technical Solutions Centers is available from http://www.nortel.com/contactus.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to http://www.nortel.com/erc.

If you purchased a Nortel service program, contact one of the following Nortel Technical Solutions Centers:

Europe, Middle East, and Africa - 00800 8008 9009 or
+44 (0) 870 907 9009

North America - (800) 4NORTEL or (800) 466-7835

Asia Pacific - (61) (2) 9927-8800

China - (800) 810-5000

Known Limitations

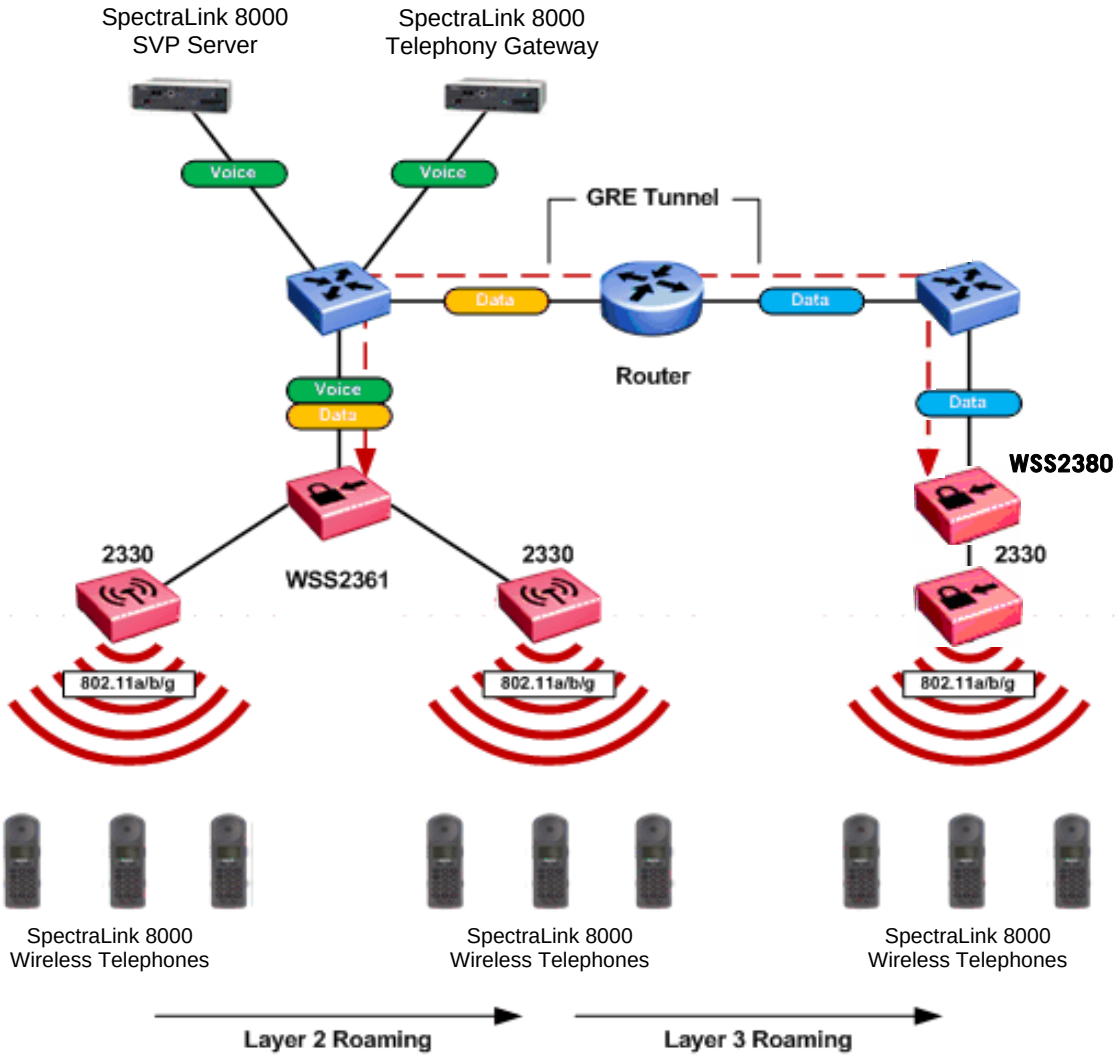
During VIEW Certification testing, the following limitations were discovered.

- RF Active Scan must be disabled on AP radios that are providing voice services, including SpectraLink 8000 Wireless Telephones.
- You must disable Internet Group Management Protocol (IGMP) snooping when running SpectraLink Radio Protocol (SRP), which is used with the SpectraLink 8000 Telephony Gateway. SRP uses multicast packets to do an SRP Check-In, which are not forwarded through the WLAN Security Switch (WSS) when IGMP snooping is enabled. When a tunneled virtual LAN (VLAN) is configured over a Layer-3 network, IGMP snooping must be disabled each time the tunnel is established, because the virtual VLAN is established with IGMP snooping turned on by default.

Network Topology

The following topology was tested during VIEW Certification. It is important to note that these do not necessarily represent all "Certified" configurations.

Both Layer-2 and Layer-3 roaming were tested. Layer-3 roaming of SpectraLink 8000 Wireless Telephones requires the use of a generic routing encapsulation (GRE) tunnel.



Access Point Capacity and Positioning

Each site is unique in its AP requirements. Therefore, please take the following points into account when determining how many APs are needed and where they should be placed in the facility:

Handset range

There must be WLAN coverage wherever the SpectraLink 8000 Wireless Telephones will be used. Adequate coverage for a SpectraLink 8000 Wireless Telephone can be determined by using the Site Survey mode on the handset that displays dBm signal levels and channel when the handset is in range of an AP.

For setting up the data rates, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. SpectraLink 8000 Wireless Telephones require the following minimum dBm reading to support the corresponding "Required" data rate setting in the access point.

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Required" Data Rate
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

All SpectraLink 8000 Wireless Telephones on the WLAN network must be configured for a single radio standard (802.11a, or 802.11b, or 802.11g). Handsets configured for different radio standards will not work together.

Number of handset calls per AP

The number of handsets that can be in-call simultaneously was determined based on call quality within a lab environment. Since call quality is impacted by packet retry rate and missed packets, test criteria were established for the maximum data rate (11Mb/s) for handsets in-range of the AP.

As the handsets move near the limits of optimal RF coverage from the AP, they will automatically drop to lower Mb/s operation. SpectraLink 8000 Wireless Telephones require approximately 15 % of

the available bandwidth per call for 1 Mb/s operation, approximately 10 % of the available bandwidth per call for 2 Mb/s operation, approximately 7 % of the available bandwidth per call for 5.5 Mb/s operation, and approximately 5 % of the available bandwidth per call for 11 Mb/s operations.

LAN bandwidth

Estimate anticipated peak call volume to ensure that the LAN has enough bandwidth to handle the network traffic generated by all of the wireless devices.

WLAN bandwidth

The SpectraLink 8000 Wireless Telephones share bandwidth with other wireless devices. To ensure adequate RF bandwidth availability, consider the number of wireless data devices in use per AP when estimating the necessary number of devices.

Configuring a New WLAN Security Switch Starting from Factory Defaults

1. Using the supplied DB-9 male to DB-9 female standard RS-232 cable, connect the WLAN Security Switch to the serial port of a terminal or PC.
2. Run a terminal emulation program (such as HyperTerminal) or use a VT-100 terminal with the following configuration:

Bits per second:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	None

3. Power-on the WLAN Security Switch. The status of the boot process will appear in the console as the switch is powering up. Once the switch is operational you will be presented with a login prompt.
4. A Quick Start Wizard provides for an easy means to perform initial WLAN Security Switch setup and configuration. Refer to the *WLAN Security Switch 2300 Series Quick Start Guide* found at Nortel's Technical Support site. This document contains a detailed explanation of using the Startup Wizard: http://support.nortel.com/go/main.jsp?cscat=DOCDETAIL&id=583095&poid=16021
5. Once the WLAN Security Switch has been configured via the Quick Start Wizard, the remaining configuration can be performed using command line interface (CLI), Web View or WLAN Management Software (WMS). Configuration examples will be provided for both CLI and WMS.
6. If necessary, the WLAN Security Switch may be reset to factory defaults. To reset the WLAN Security Switch to factory defaults, you must issue the "clear boot config" command via the console.

Connecting APs

To configure the WLAN Security Switch (WSS) to support an AP, you must first determine how the AP will connect to the switch. There are two types of AP-to-WSS connection: direct and distributed.

Directly connected APs

In direct connection, an AP connects to one or two 10/100 ports on a WSS. The WSS port is then configured specifically for a direct attachment to an AP. There is no intermediate networking equipment between the WSS and AP, and only one AP is connected to the WSS port. The WSS 10/100 port provides power over Ethernet (PoE) to the AP. The WSS also forwards data only to and from the configured AP on that port. The port numbers on the WSS which are configured for directly attached APs reference a particular AP.

Distributed APs

An AP that is not directly connected to a WSS is considered a distributed AP. There may be intermediate Layer 2 switches or Layer 3 IP routers between the WSS and the AP. The WSS may communicate to the distributed AP through any network port. (A network port is any port connecting the switch to other networking devices, such as switches and routers, and it can also be configured for 802.1Q VLAN tagging.) The WSS contains a configuration for a distributed AP based on the AP's serial number. Similar to ports configured for directly connected APs, distributed AP configurations are numbered and can reference a particular AP. These numbered configurations do not, however, reference any physical port.

During VIEW Certification, the 2330 access points were tested while directly connected to a port on the WLAN Security Switch (e.g. port 1), but both methods are supported.

For more information on how to configure the network to support a distributed AP, see the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.

Command, comment, and screen text key

In the sections below you will find commands, comments and system responses or other screen-displayed information involved in the configuration process. This key explains the text styles and symbols used to denote them.

Text Style	Denotes:
xxxxxxxx	Typed command
<xxxxxxxx>	Encryption key, domain name or other information specific to your system that needs to be entered
# xxxxxxxx	Comment about a command or set of commands
xxxxxxxx	System response or other displayed information

Configuration Example – CLI

AP configuration

To add a directly connected AP-2330 attached to port 1 on a WSS using CLI:

```
set port type ap 1 model 2330 poe enable
   # Defines the port number on the switch that the AP
   is connected to, the model number of the AP and
   enables PoE on the switch port. Valid model numbers
   include the 2330, 2330A and 2330B.
set ap 1 radio 1 tx-power 10 mode enable
   # Sets the channel number, transmit power and enables
   the 802.11g radio.
set ap 1 radio 2 channel 44 tx-power 10 mode enable
   # Sets the channel number, transmit power and enables
   the 802.11a radio.
```

To add a distributed AP-2330 to a WSS using CLI:

```
set dap 1 serial-id stpw20kc3 model 2330
   # Defines the DAP number, serial-id and model number
   of the AP. Valid model numbers include the 2330,
   2330A and 2330B.
set dap 1 radio 1 channel 11 tx-power 10 mode enable
   # Sets the channel number, transmit power and enables
   the 802.11g radio.
set dap 1 radio 2 channel 40 tx-power 10 mode enable
   # Sets the channel number, transmit power and enables
   the 802.11a radio.
```

VLAN configuration

For security and flexibility it is recommended that voice and data be configured on separate VLANs. For this example a new VLAN named Voice with a VLAN ID 2 will be created and tagged to the uplink port 8:

```
set vlan 2 name Voice
   # Creates a new VLAN ID and defines the name.
set vlan 2 port 8 tag 2
   # Assigns the VLAN to a port and specifies an 802.1Q
   tag value.
set igmp disable vlan Voice
   # Disables IGMP on Voice VLAN.
```

Service profile / SSID configuration

To create a SSID named Voice using WPA-PSK that will be advertised on 802.11a/b/g radios using CLI:

```
set service-profile Voice ssid-name Voice
   # Creates a new service profile and SSID named Voice. Note it's a best practice recommendation to use the same name for both the service profile and SSID
set service-profile Voice auth-fallthru last-resort
   # Sets the authentication type to open authentication. With WPA-PSK the pre-shared key will be used to authenticate the handset.
set service-profile Voice wpa-ie enable
   # Enables WPA security.
set service-profile Voice psk-phrase <enter-a-passphrase>
   # Defines the passphrase required to access the SSID.
set service-profile Voice auth-psk enable
   # Enables pre-shared-key authentication.
set service-profile Voice auth-dot1x disable
   # Disables 802.1x authentication.
set service-profile Voice attr vlan-name Voice
   # Specifies the VLAN name to map the voice handsets traffic to.
```

To create a SSID named Voice using WPA2-PSK that will be advertised on 802.11a/b/g radios using CLI:

```
set service-profile Voice ssid-name Voice
   # Creates a new service profile and SSID named Voice. Note it's a best practice recommendation to use the same name for both the service profile and SSID
set service-profile Voice auth-fallthru last-resort
   # Sets the authentication type to open authentication. With WPA-PSK the pre-shared key will be used to authenticate the handset.
set service-profile Voice rsn-ie enable
   # Enables WPA2 security.
set service-profile Voice cipher-tkip disable
   # Disables TKIP encryption.
set service-profile Voice cipher-ccmp enable
   # Enables AES/CCMP encryption.
set service-profile Voice psk-phrase <enter-a-passphrase>
   # Defines the passphrase required to access the SSID.
set service-profile Voice auth-psk enable
   # Enables pre-shared-key authentication.
```

```
set service-profile Voice auth-dot1x disable
   # Disables 802.1x authentication.
set service-profile Voice attr vlan-name Voice
   # Specifies the VLAN name to map the voice handsets
   traffic to.
```

Radio Profile configuration

The default Radio Profile needs to be modified to disable certain features to support the handsets. To modify the default Radio Profile using CLI:

```
set radio-profile default service-profile Voice
   # Maps the voice service profile and SSID to the
   radio profile. This determines which 802.11 radios
   advertise and can support voice handsets.
set radio-profile default dtim-interval 3
   # Sets the DTIM interval to support push-to-talk.
set radio-profile default auto-tune channel-config
disable
   # Disables automatic channel assignment for radios
   assigned to the radio profile. A static channel
   configuration is recommended to provide a stable and
   optimum RF environment for the handsets.
set radio-profile default active-scan disable
   # Disables active-scanning which prevents the radios
   from going off-channel and disrupting voice services.
set radio-profile default qos-mode svp
   # Sets the QoS mode to SVP. WMM support is not
   currently available on the SpectraLink 8000 Wireless
   Telephones.
```

Access control list

To create an access control list (ACL) that allows and prioritizes IP protocol 119 (SVP) with a Class of Service (CoS) 7 and allows all other IP traffic on the Voice VLAN using CLI:

```
set security acl ip SpectraLink permit cos 7 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
   # Creates an ACL that matches protocol 119 (SVP) and
   marks it with a CoS 7.
set security acl ip SpectraLink permit 0.0.0.0
255.255.255.255
   # Creates an ACL that matches all traffic and ports.
commit security acl SpectraLink
   # Commits and applies the ACL.
set security acl map SpectraLink vlan Voice in
set security acl map SpectraLink vlan Voice out
```

```
   # Applies the ACL to the Voice VLAN for ingress and
   egress traffic.
```

To create an ACL that allows and prioritizes IP protocol 119 (SVP) with a Class of Service (CoS) 7 and denies all other IP traffic on the Voice VLAN using CLI:

```
set security acl ip SpectraLink permit cos 7 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
   # Creates an ACL that matches protocol 119 (SVP) and
   marks it with a CoS 7
commit security acl SpectraLink
   # Commits and applies the ACL.
set security acl map SpectraLink vlan Voice in
set security acl map SpectraLink vlan Voice out
   # Applies the ACL to the Voice VLAN for ingress and
   egress traffic.
```

Saving changes

To save the current changes to a WSS using CLI:

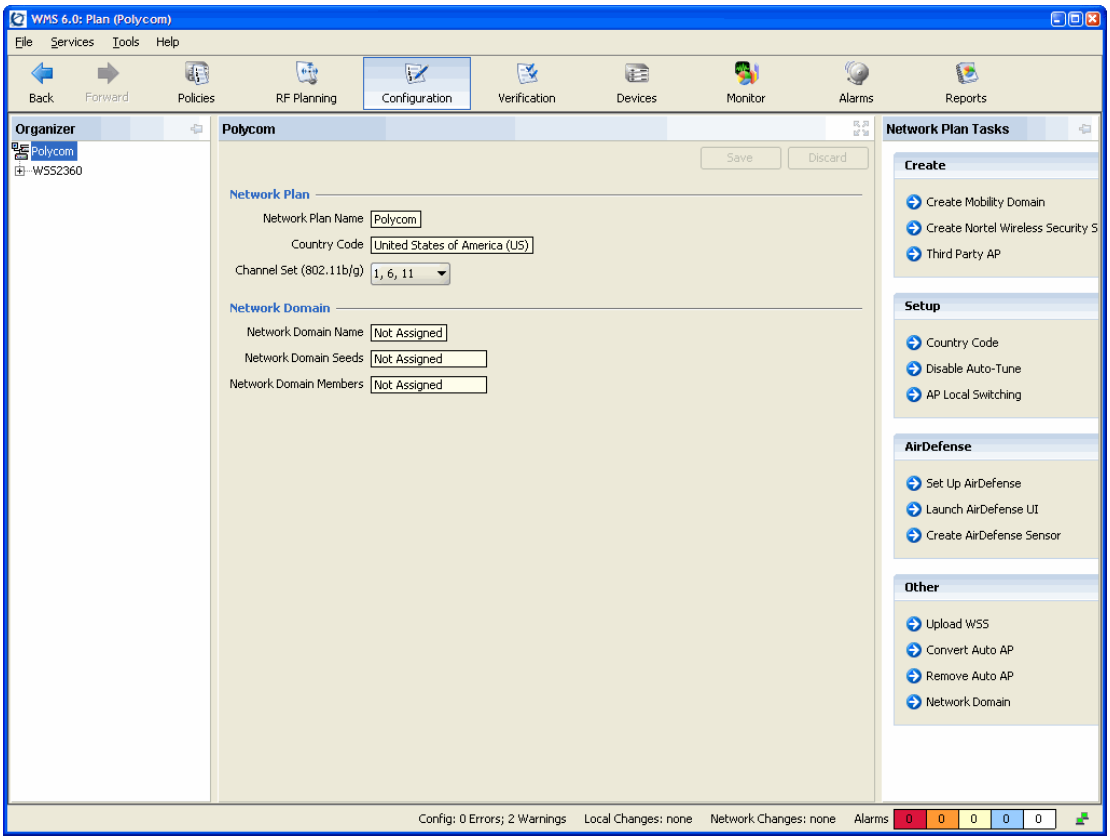
```
save config
   # Saves all configuration changes to the running
   configuration file.
```

Configuration Example – WLAN Management Software

Adding a WLAN Security Switch to the Network Plan

Before WLAN Management Software can be used to configure a WLAN Security Switch, the WSS must be added to the WMS server. To add a WLAN Security Switch to WLAN Management Software:

1. Assuming that WMS is installed and a Network Plan has been created, launch the WMS client and connect to the WMS server. For more information, see the *Nortel WLAN Management Software 2300 Series User Guide*.
2. In WMS, click **Configuration** on the tool bar.
3. In the **Network Plan Tasks** panel, under **Other** select **Upload WSS**.



4. In the **IP Address** field, type the IP address for the WLAN Security Switch.

5. In the **Enable Password** field, type the enable password for the WLAN Security Switch.

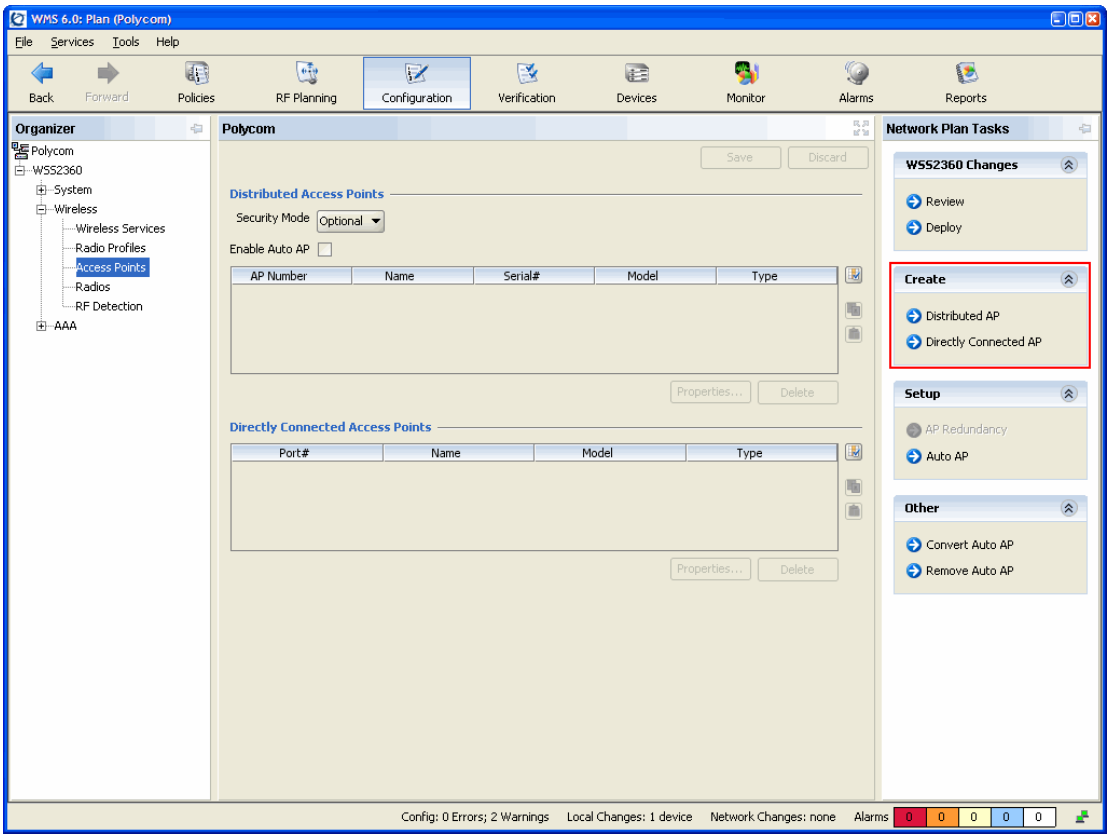
The enable password must match the enable password that was defined in the Quick Start Wizard. For more information, see the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.

6. Click the **Next** button. The uploading progress is shown.
7. After the **Successfully uploaded device** message is displayed, click the **Next** button.

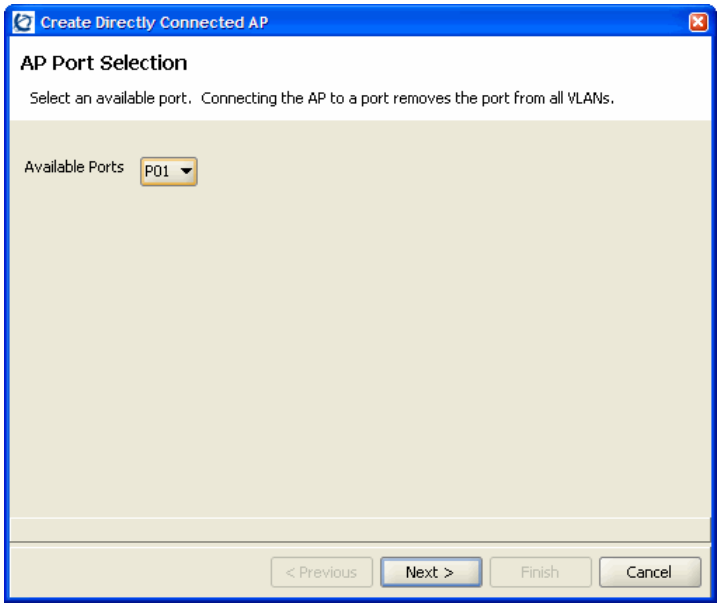
AP configuration

To add a directly connected or distributed AP to a WLAN Security Switch using WMS:

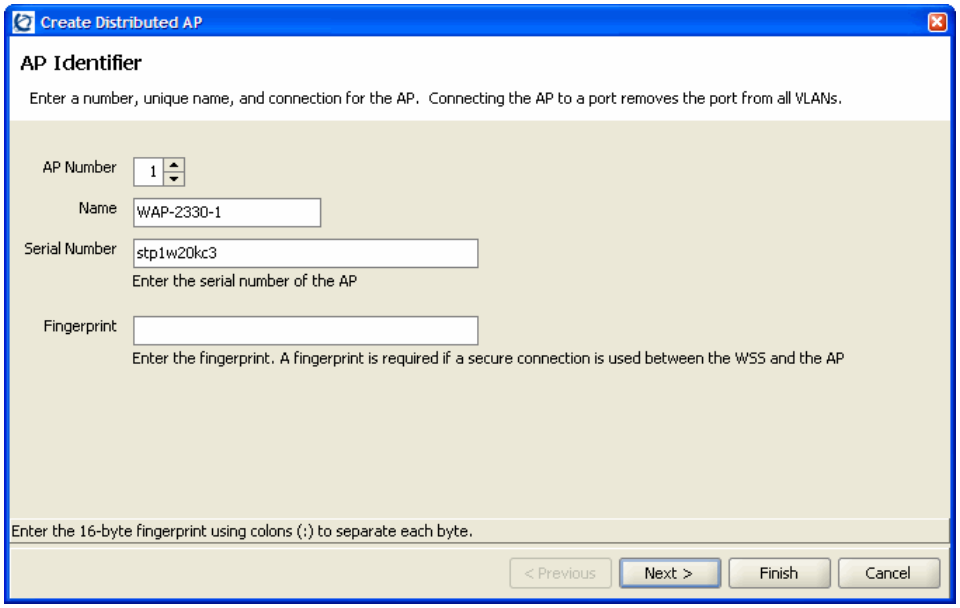
1. Connect the AP to the network (distributed AP) or a free PoE port on the switch (directly connected AP).
2. In WMS click **Configuration** on the tool bar.
3. In the **Organizer** panel, expand the **WSS** and select **Access Points**.
4. In the **Network Plan Tasks** panel, create a new AP by selecting **Distributed AP** or **Directly Connected AP**.



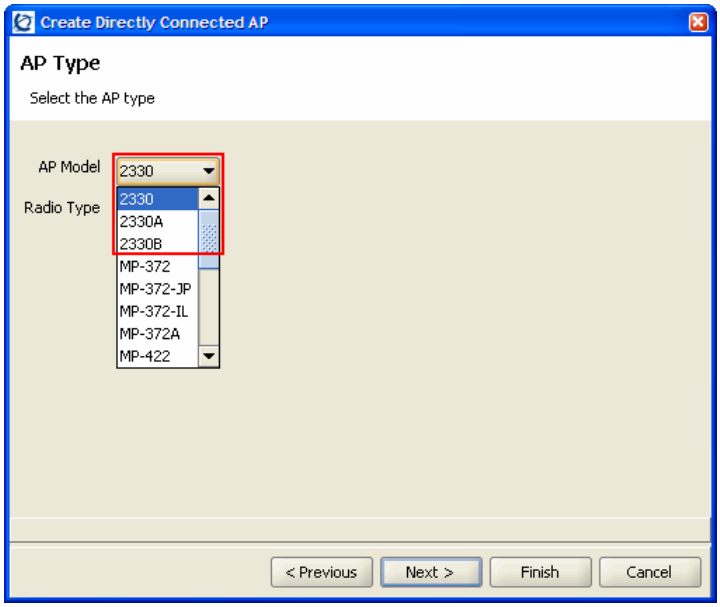
5. For directly connected APs, select an available port on the switch from the **Available Ports** drop-down list. Click the **Next** button.



6. For distributed APs, enter the **Name** and **Serial Number** of the AP. Click the **Next** button.



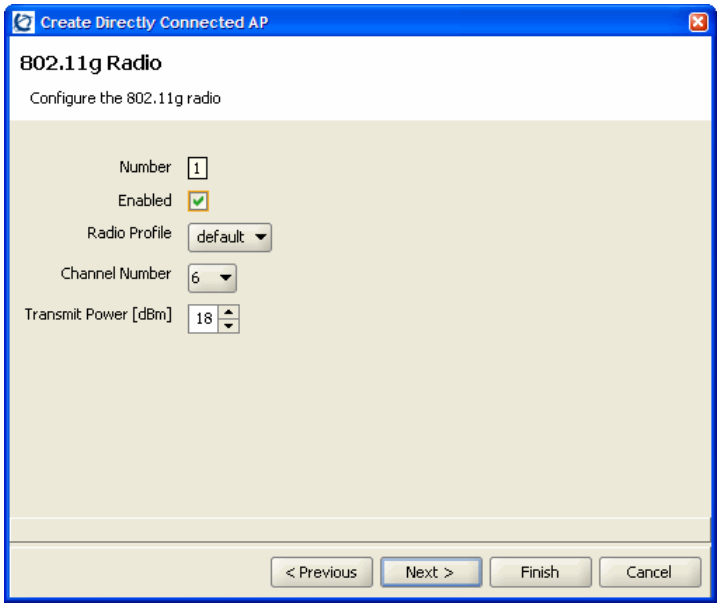
7. Specify the model of the Nortel AP you are configuring. Valid models include **2330, 2330A** and **2330B**. Click the **Next** button.



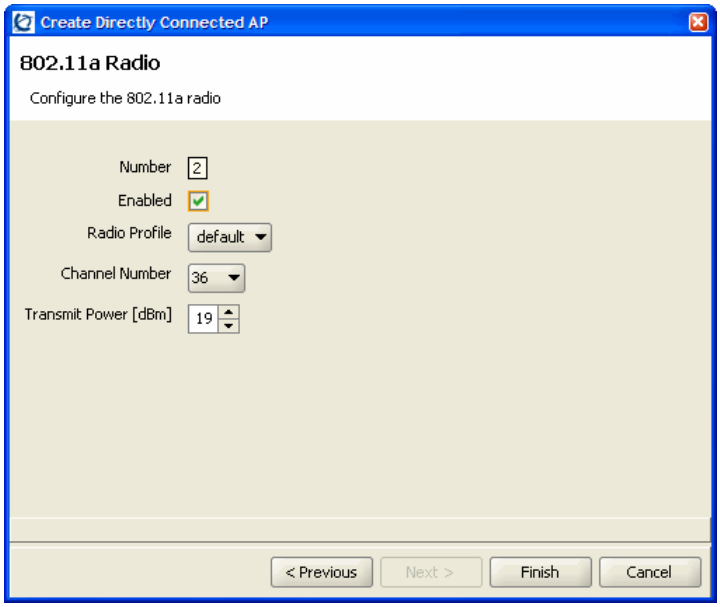
8. To configure the **802.11g Radio**:

   a. Select **default** for the **Radio Profile**.

   b. Specify the **Channel Number** and **Transmit Power** the radio should use, as determined by the site survey performed on the facility. Click the **Next** button.



9. To configure the **802.11a Radio**,
   a. Select **default** for the **Radio Profile**.
   b. Specify the **Channel Number** and **Transmit Power** the radio should use, as determined by the site survey performed on the facility.
10. Click the **Finish** button.

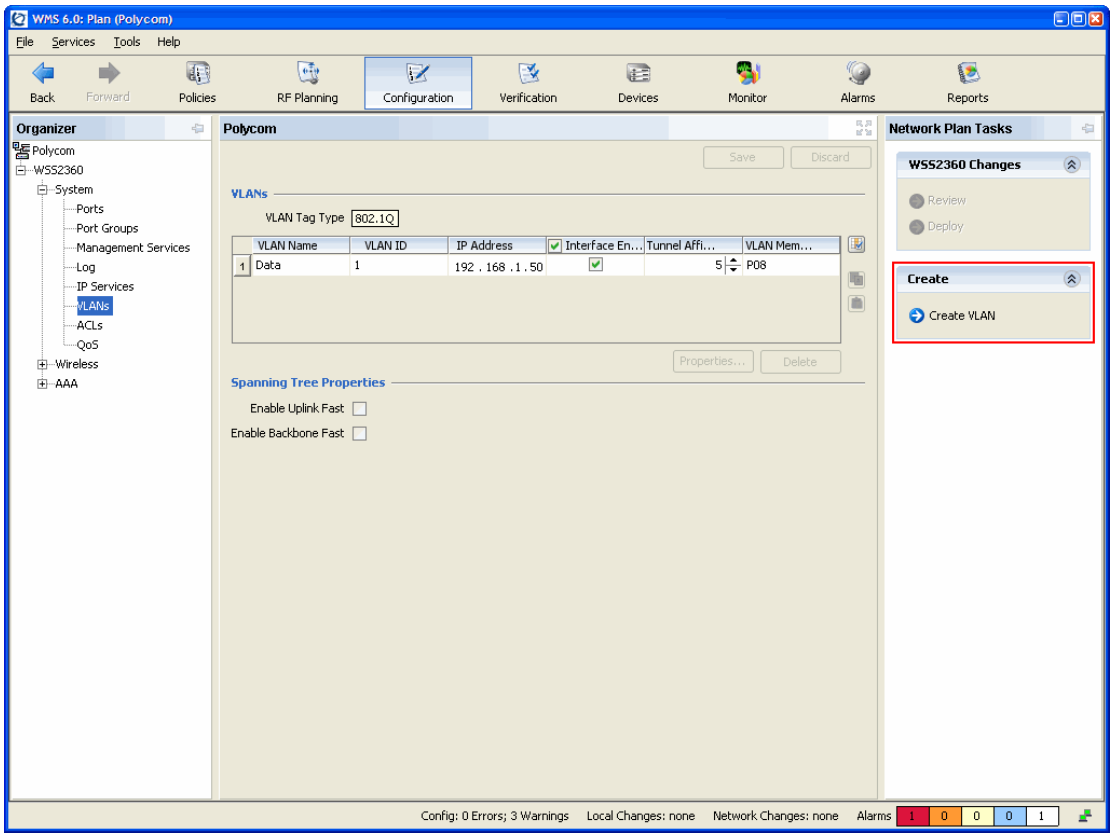


11. The AP has now been added to the WLAN Security Switch.

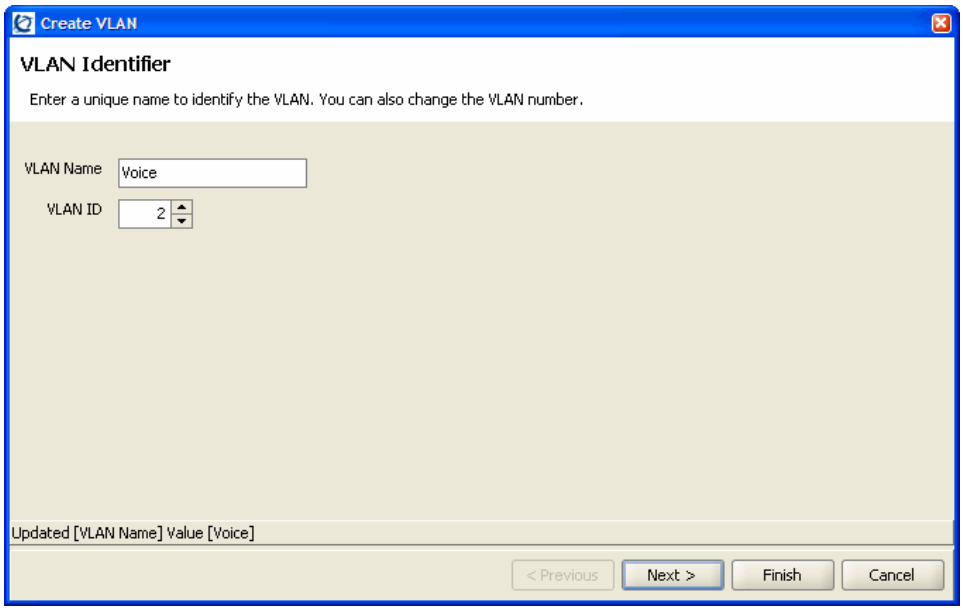
VLAN configuration

For security and flexibility it is recommended that voice and data be on separate VLANs. For this example, a new VLAN named **Voice** with a VLAN ID **2** will be created and tagged to the uplink port **8**.

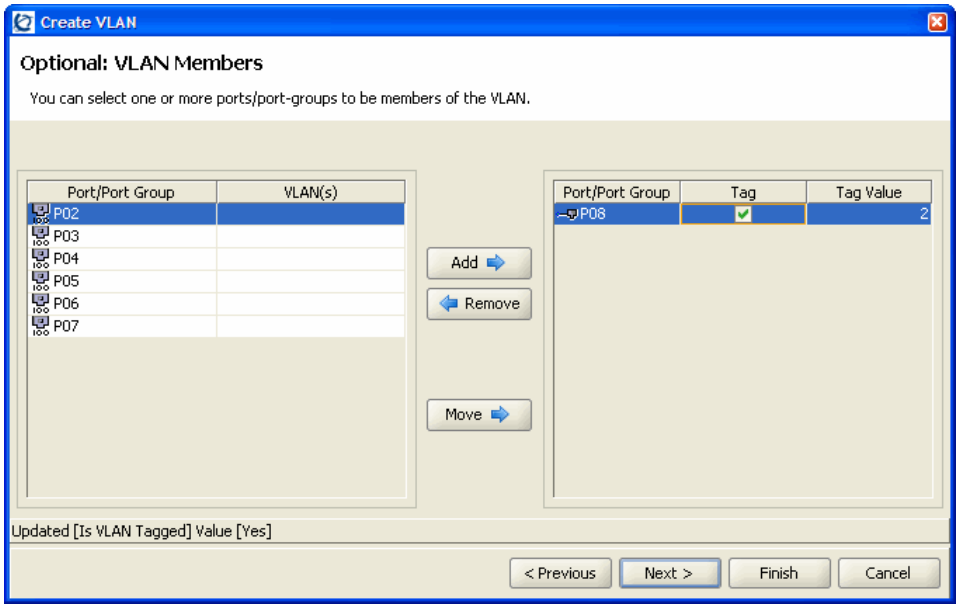
1. In WMS click **Configuration** on the tool bar.
2. In the **Organizer** panel, expand the **WSS** and select **VLANs**.
3. In the **Network Plan Tasks** panel, select **Create VLAN.**



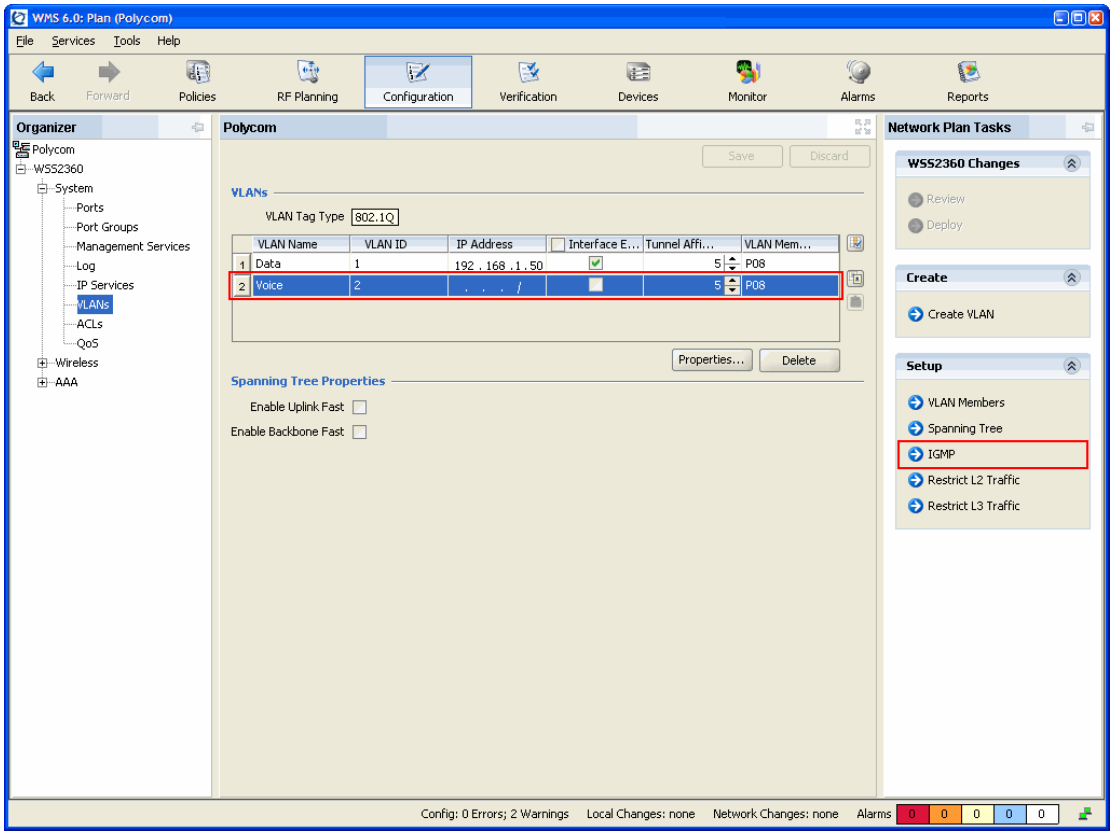
4. For **VLAN Name** enter **Voice**.
5. For **VLAN ID** specify **2**. Click the **Next** button.



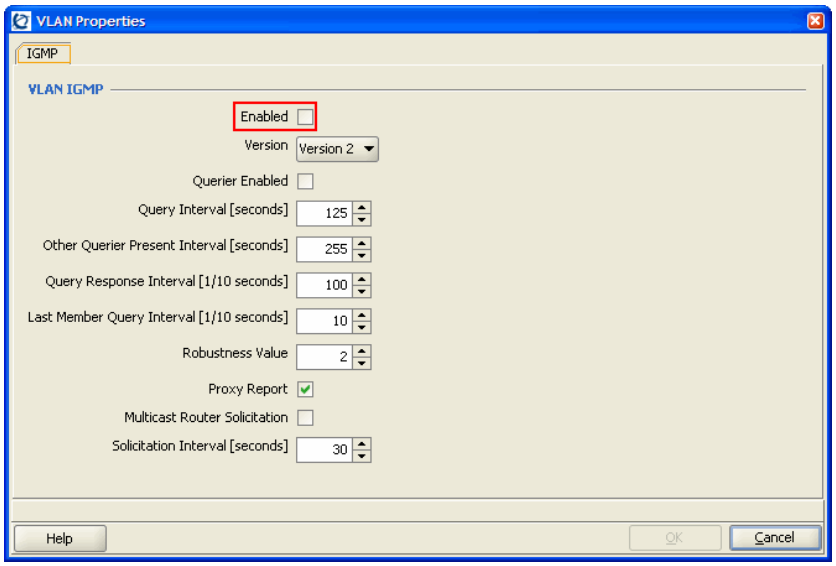
6. In the **Port/Port Group** list, select the 802.1Q tagged uplink port **(P08)** and click the **Add** button.
7. Click the **Tag** check box and specify the 802.1Q tag value **2**.
8. Click the **Finish** button.



9. The Voice VLAN 2 is now 802.1Q tagged to the uplink port P08.
   a. Highlight the **Voice** VLAN.
   b. In the **Network Plan Tasks** panel, select **IGMP.**



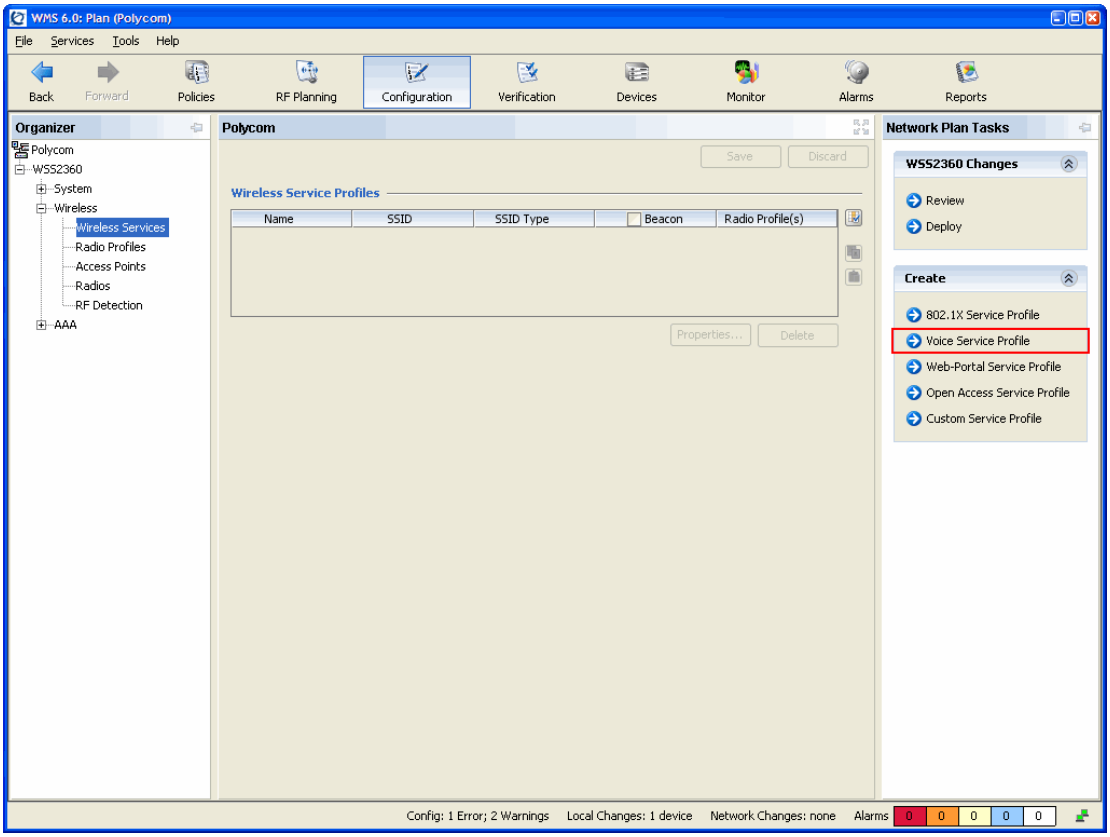
10. In the **VLAN Properties** window, disable IGMP by clearing the **Enabled** check box. Click the **OK** button.



Service Profile / SSID configuration

To create a SSID named **Voice** using **WPA-PSK** or **WPA2-PSK** that will be advertised on 802.11a/b/g radios using WMS:

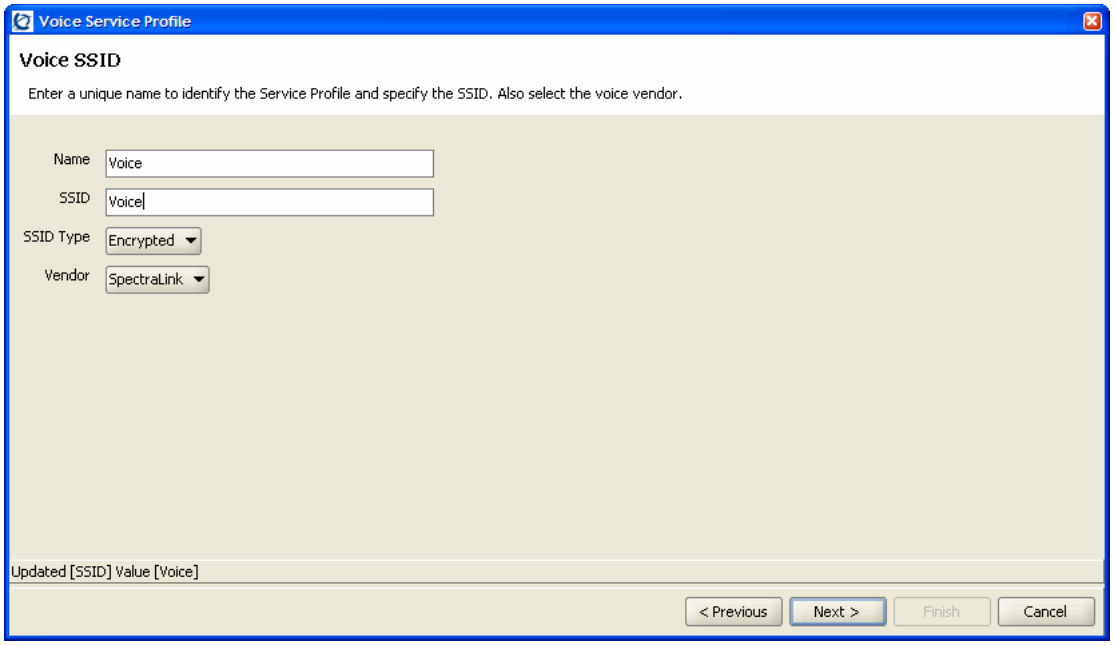
1. In WMS click **Configuration** on the tool bar.
2. In the **Organizer** panel expand the **WSS** and select **Wireless Services**.
3. In the **Network Plan Tasks** panel, create a new wireless service by selecting **Voice Service Profile**.



4. In the **New Voice Service Profile** introduction screen click the **Next** button.
5. Specify a **Name** and **SSID** for the **Voice Service Profile.**

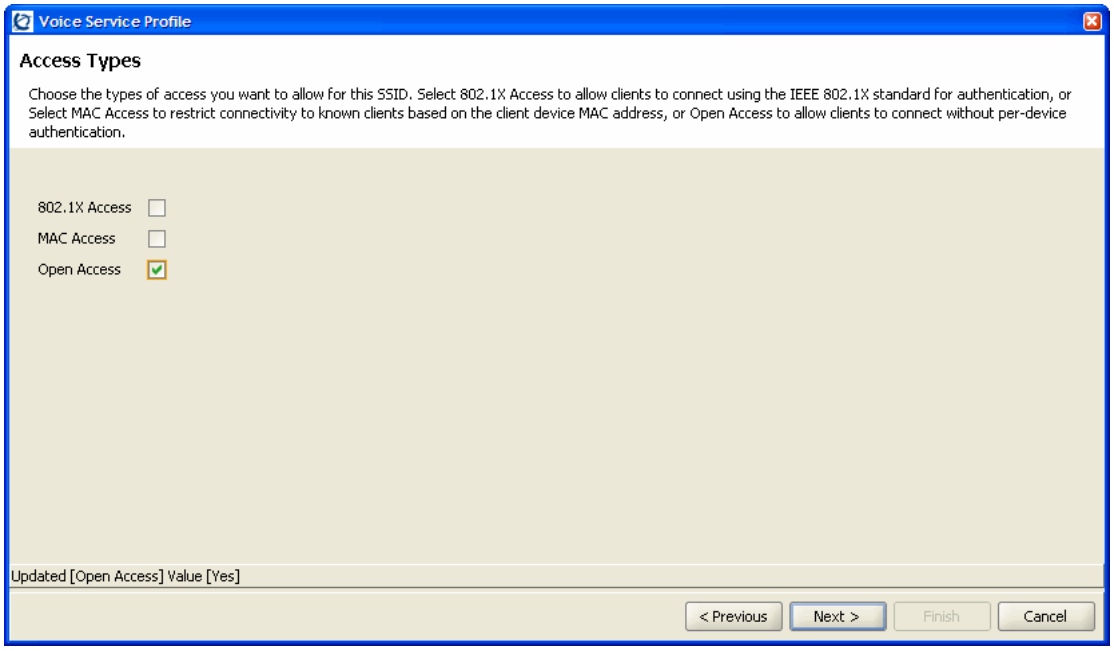
6. Set the **SSID Type** to **Encrypted** and use the default **Vendor** type **SpectraLink**. Click the **Next** button.

Selecting the vendor **SpectraLink** tells WMS what ACLs to create to prioritize the voice traffic later in the wizard.



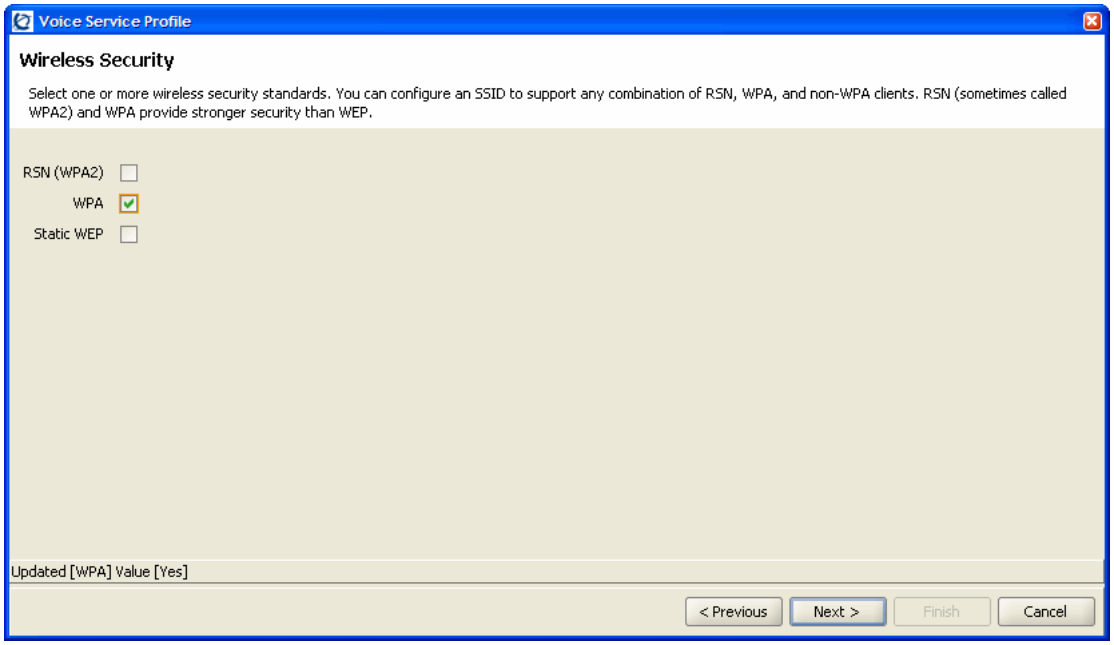
7. Select the **Open Access** check box. Click the **Next** button.

MAC authentication may optionally be selected but will require that the MAC addresses for each handset be defined in the local AAA database on the WSS.

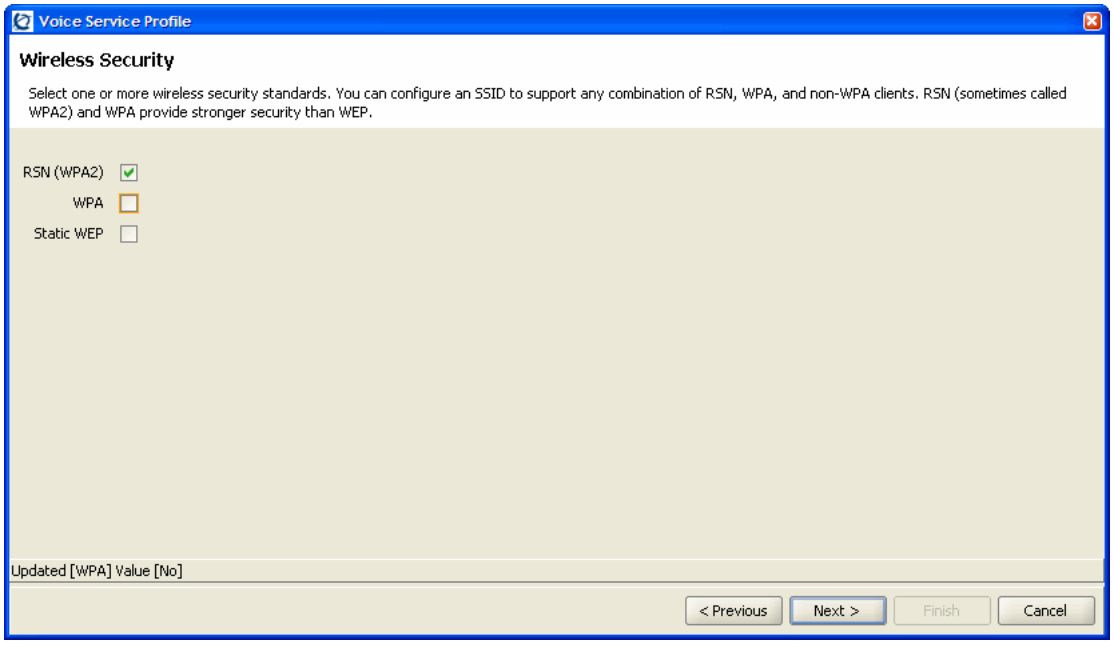


8. Settings for **Wireless Security**:

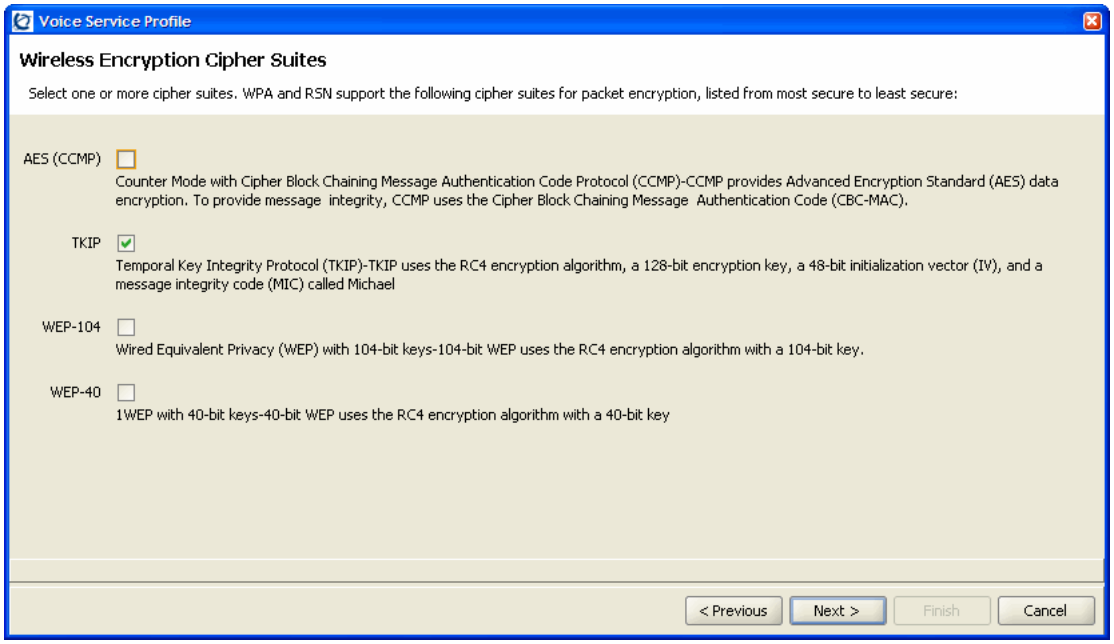
   a. To support handsets using WPA-PSK security, select the **WPA** check box.



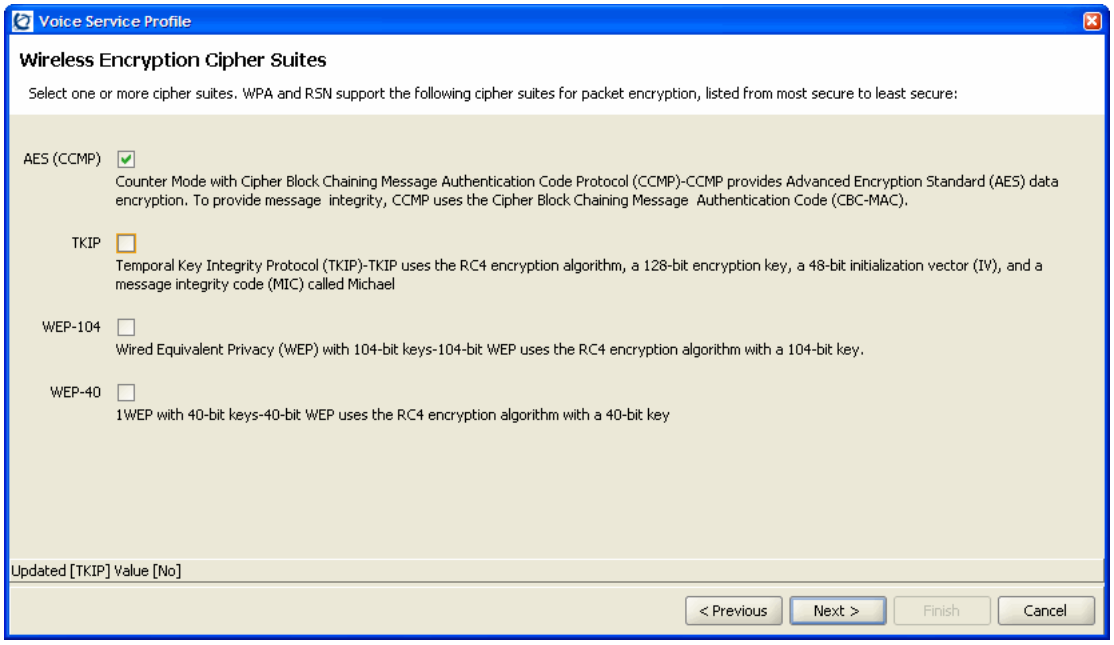
   b. To support handsets using WPA2-PSK, select the **RSN (WPA2)** check box.



9. Click the **Next** button.
10. Settings for **Wireless Encryption Cipher Suite**:
    a. To support handsets using WPA-PSK with TKIP, select the **TKIP** check box.



b. To support handsets using WPA2-PSK with AES/CCMP, select the **AES (CCMP)** check box.



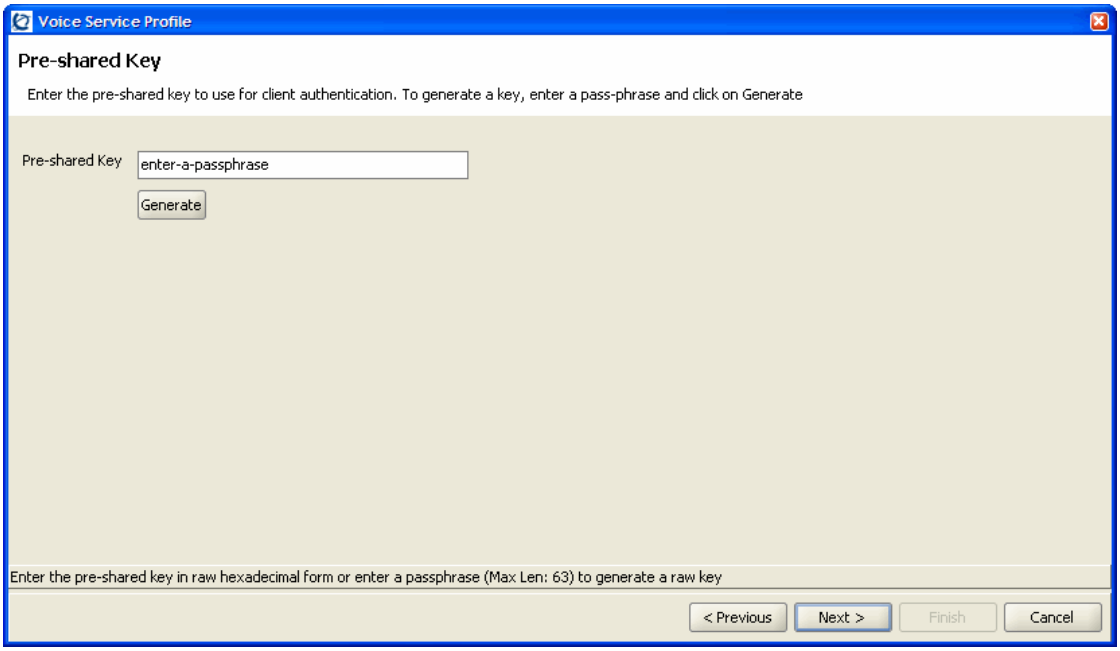
11. Click the **Next** button.

12. Enter a hexadecimal pre-shared key or passphrase.

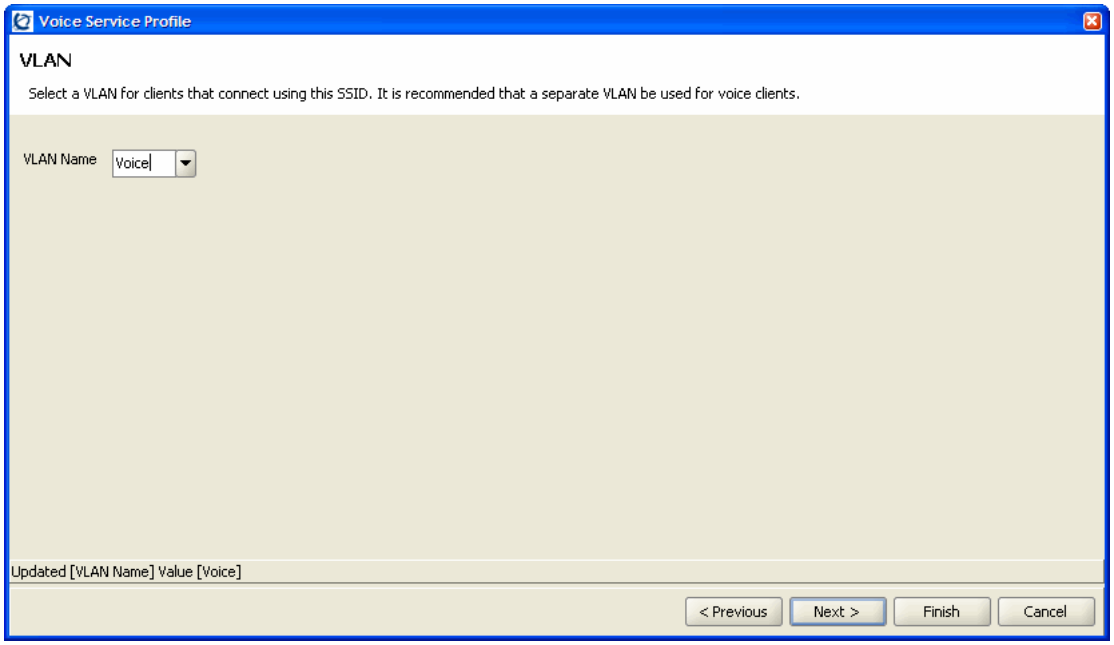
    a. If a passphrase is entered, click the **Generate** button to generate the hexadecimal pre-shared key.

13. Click the **Next** button.

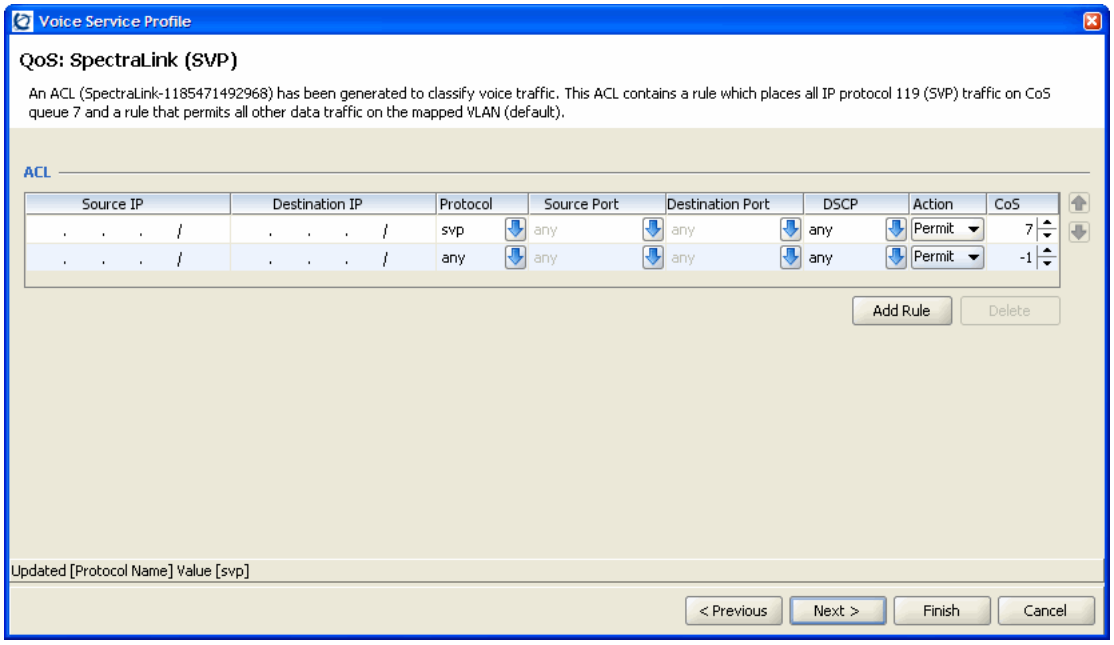
The pre-shared key must match on both the WSS and handsets or the handsets will not be able to associate with the Voice SSID.



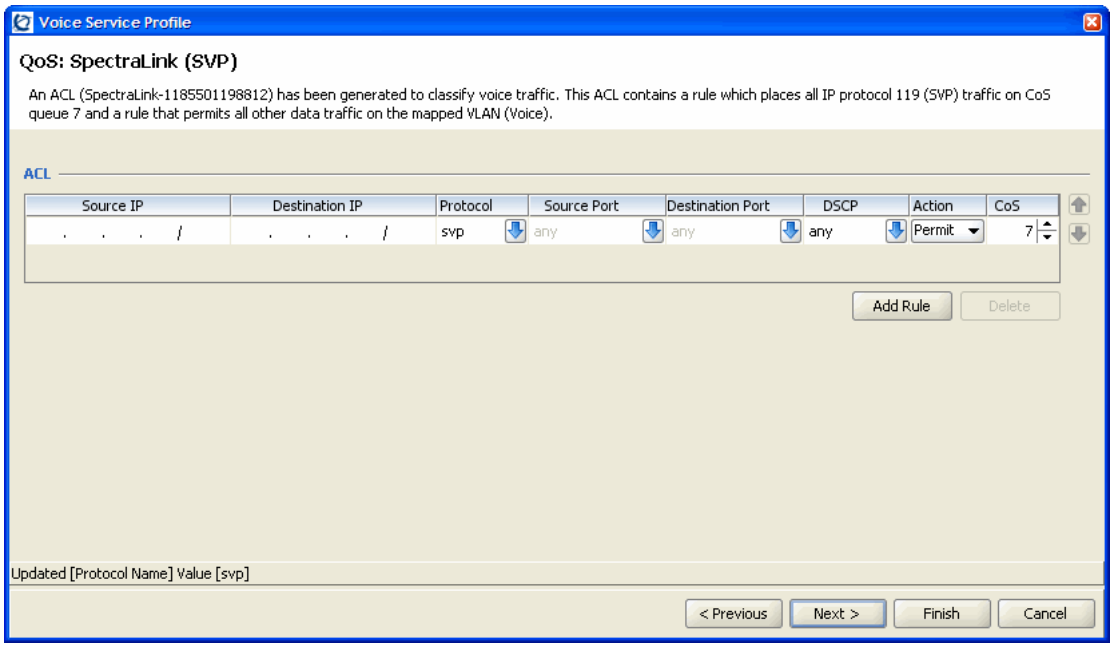
14. Specify the VLAN named **Voice**. This determines the VLAN that the WSS will map the handset traffic to. Click the **Next** button.



15. A default ACL will be generated which will allow and prioritize IP protocol 119 (**SVP**) traffic with the Class of Service level **7** and pass all other IP traffic on the Voice VLAN.



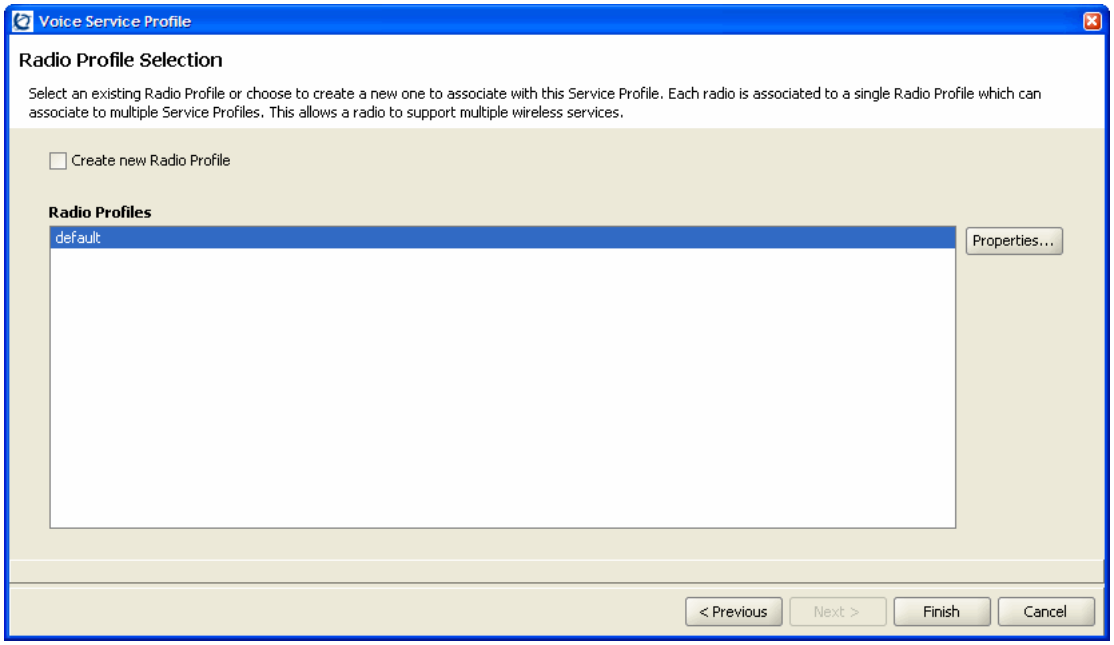
a. (Optional) Modify the default ACL by removing the last statement, which will allow and prioritize IP protocol 119 (SVP) but deny all other IP traffic on the Voice VLAN. Click the **Next** button.



16. Assign the **Voice Service Profile** to the **default** Radio Profile. This will determine which 802.11a and 802.11g radios will advertise the Voice SSID. For this example the default Radio Profile will be used which is assigned to all 802.11a/g radios. This will provide support for handsets operating in 802.11a, 802.11b and 802.11g modes.

All SpectraLink 8000 Wireless Telephones on the WLAN network must be configured for a single radio standard (802.11a, or 802.11b, or 802.11g). Handsets configured for different radio standards will not work together.

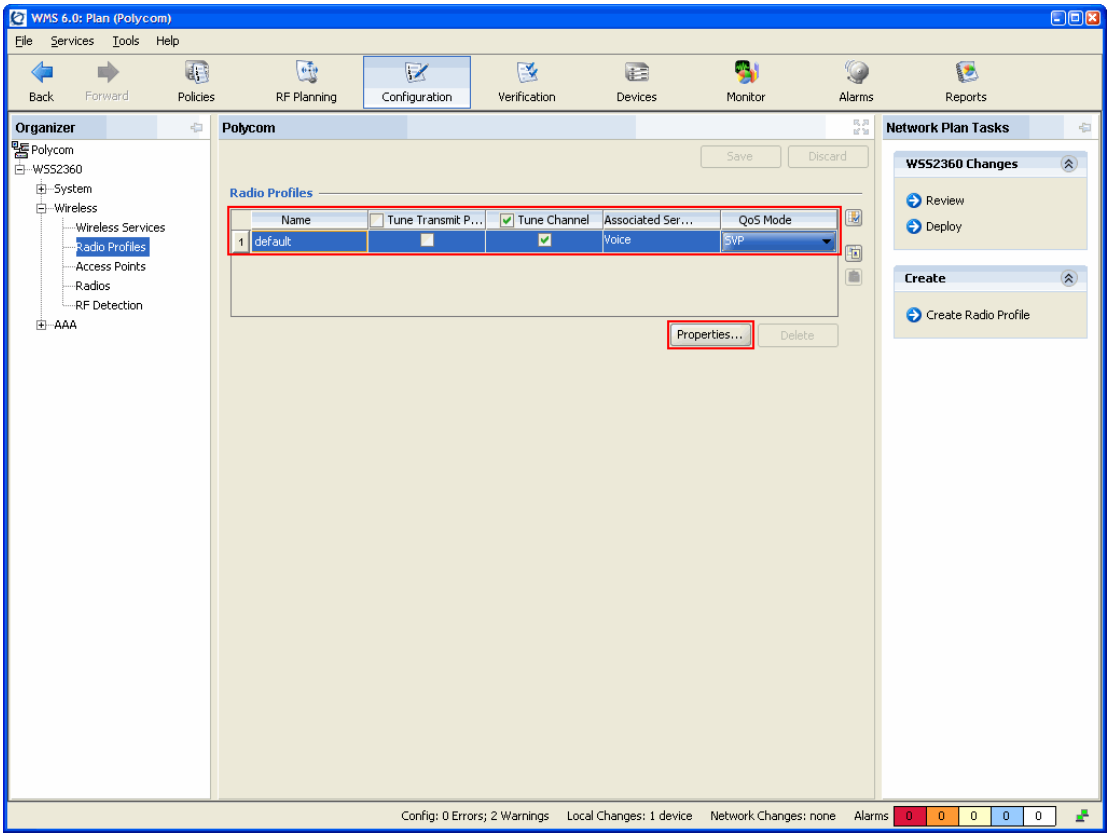
17. Click the **Finish** button.
A Voice Service Profile to support the handsets has now been added to the WSS configuration in WMS.



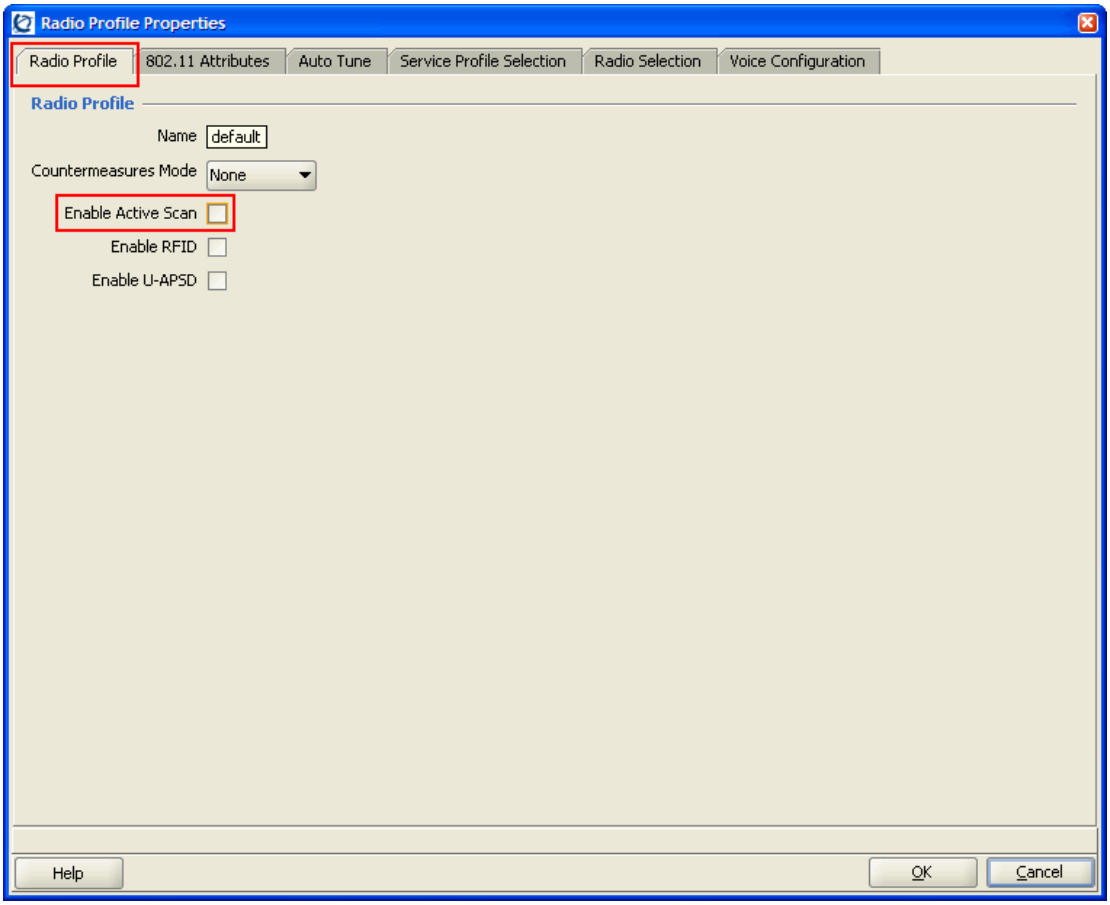
Radio Profile configuration

The default Radio Profile needs to be modified to disable certain features to support the handsets. To modify the default Radio Profile using WMS:

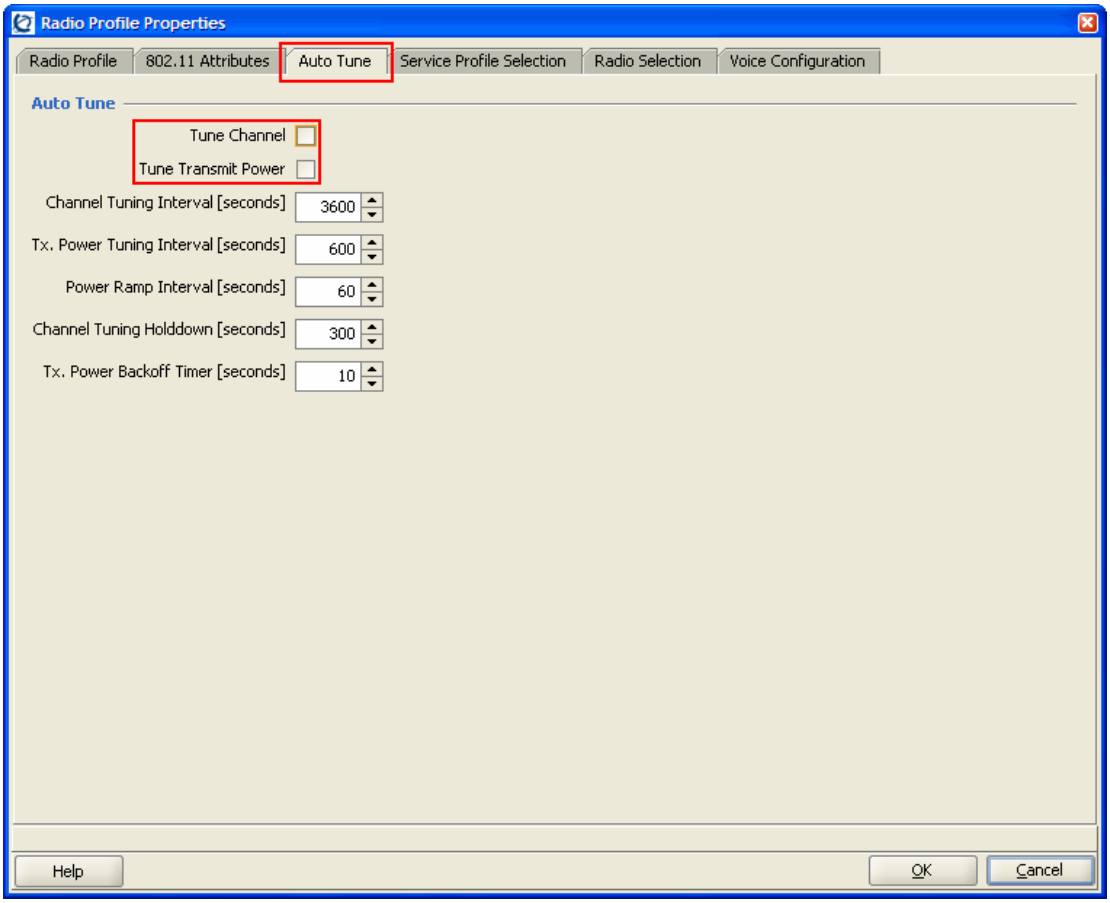
1. In WMS click **Configuration** on the tool bar.
2. In the **Organizer** panel expand the **WSS** and select **Radio Profiles.**
3. In the **Radio Profiles** list, highlight the **default** Radio Profile and click the **Properties** button.



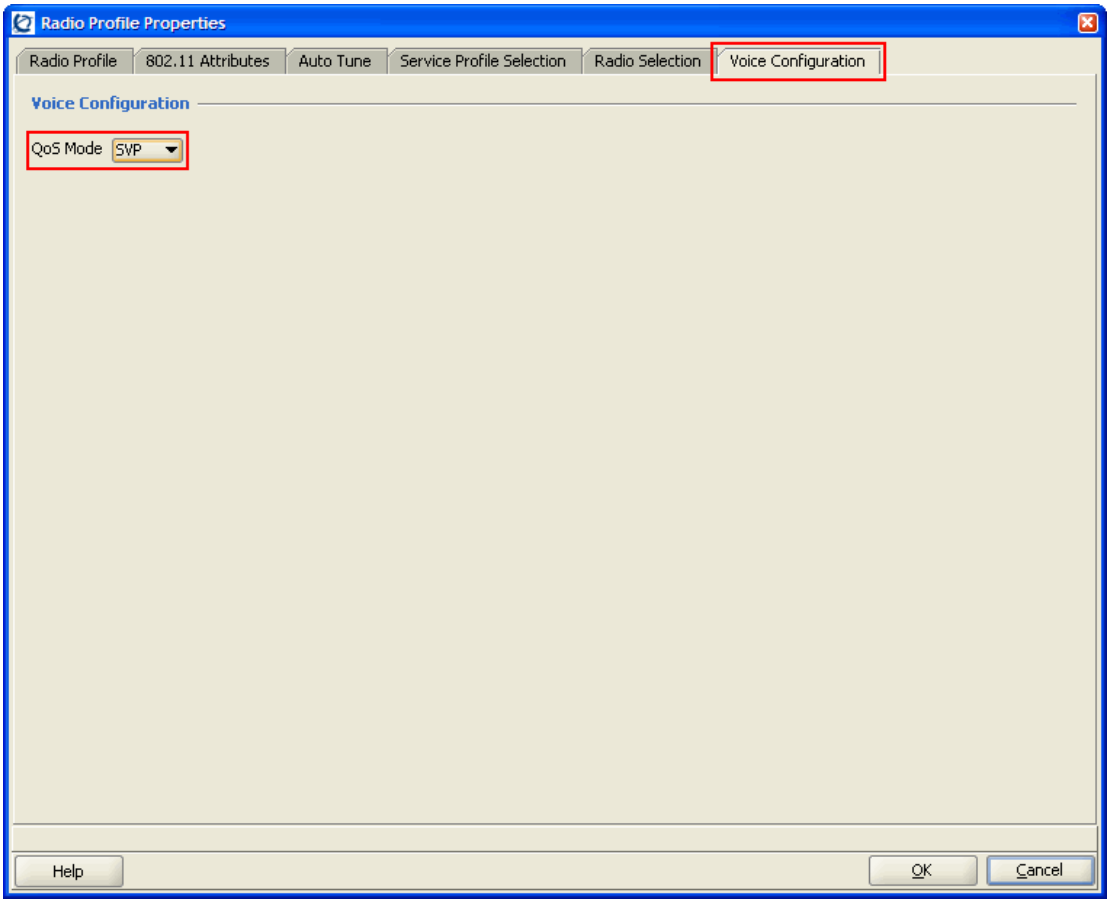
4. In the **Radio Profile Properties** window, click the **Radio Profile** tab.
5. Clear the **Enable Active Scan** check box. This disables active scanning, which prevents the radios from going off-channel and disrupting voice services.



6. Click the **Auto Tune** tab.
7. Clear the **Tune Channel** and **Tune Transmit Power** check boxes. This disables automatic channel assignment for radios assigned to the radio profile. A static channel configuration is recommended to provide a stable and optimum RF environment for the handsets.



8. Click the **Voice Configuration** tab. Verify that the **QoS Mode** is set to **SVP**. WMM support is not currently available on the SpectraLink 8000 Wireless Telephones.
9. Click the **OK** button.

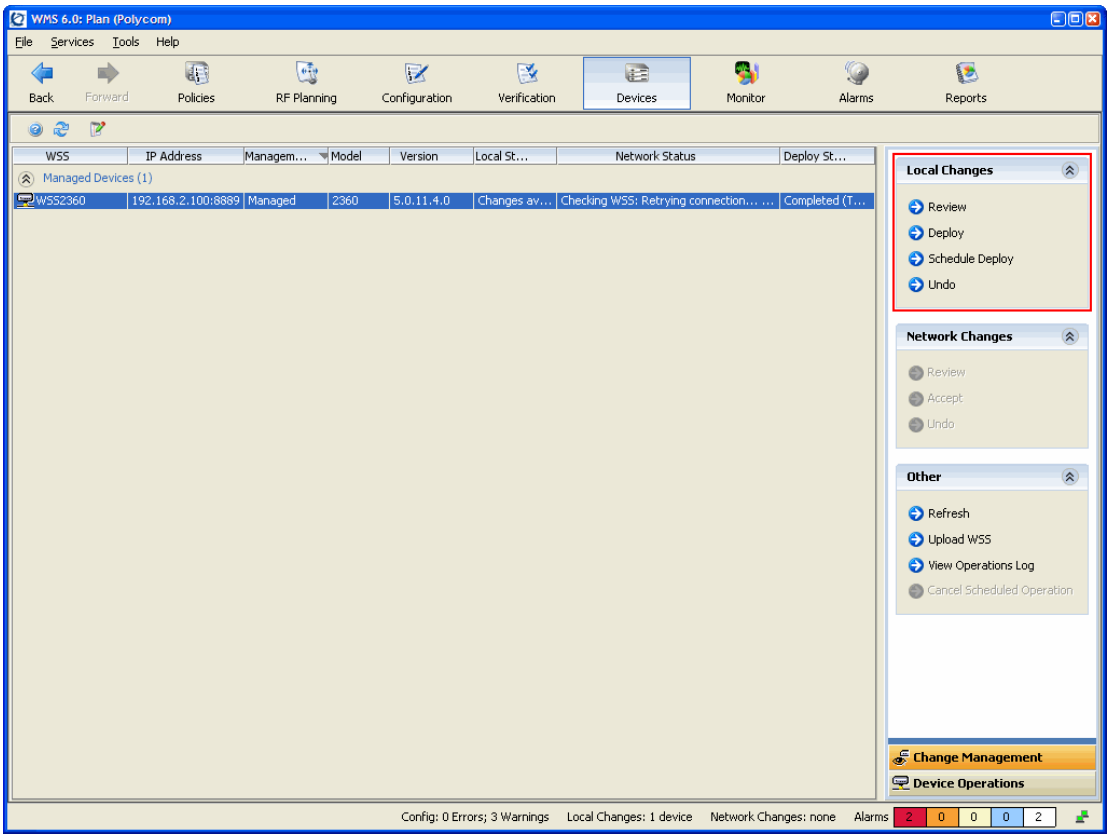


Deploying changes

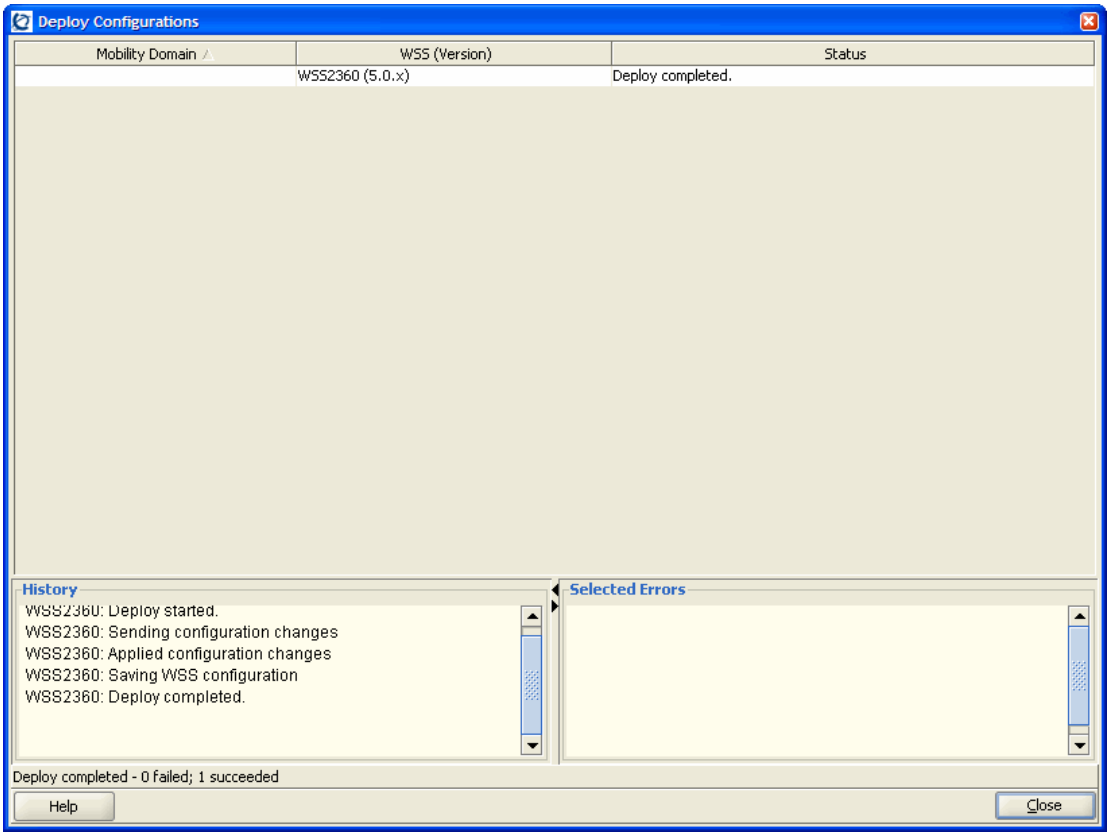
Deploying the changes in WMS will upload and save the configuration to the WSS. To deploy the changes in WMS:

1. In WMS click **Devices** on the tool bar.
2. In the **Local Changes** Task List panel, select **Deploy** to upload and save the configuration changes to the WSS.

You may also **Review**, **Schedule** and **Undo** changes in the **Local Changes** Task List panel.



3. When the **Deploy** option is selected, WMS will send, apply and save the configuration changes to the WSS.



Example Configuration Files (For Reference Only)

The following configuration file provides an example configuration to support SpectraLink 8000 Wireless Telephones using WPA-PSK:

```
# Configuration nvgen'd at 2007-7-26 22:51:55
# Image 5.0.11.4.0
# Model 2360
# Last change occurred at 2007-7-26 22:36:12
set ip route default 192.168.1.1 1
set system name WSS2360
set system ip-address 192.168.1.50
set system countrycode US
set timezone EST -5 0
set service-profile Voice ssid-name Voice
set service-profile Voice auth-fallthru last-resort
set service-profile Voice wpa-ie enable
set service-profile Voice psk-phrase enter-a-passphrase
set service-profile Voice auth-psk enable
set service-profile Voice auth-dot1x disable
set service-profile Voice attr vlan-name Voice
set enablepass password enable-password
set user admin password admin-password
set radio-profile default service-profile Voice
set radio-profile default dtim-interval 3
set radio-profile default auto-tune channel-config
disable
set radio-profile default active-scan disable
set radio-profile default qos-mode svp
set dap 1 serial-id stpw20kc3 model 2330
set dap 1 name WAP-2330-2
set dap 1 radio 1 channel 11 tx-power 10 mode enable
set dap 1 radio 2 channel 40 tx-power 10 mode enable
set port type ap 1 model 2330 poe enable
set ap 1 name WAP-2330-1
set ap 1 radio 1 tx-power 10 mode enable
set ap 1 radio 2 channel 44 tx-power 10 mode enable
set ip https server enable
set port poe 1 enable
set vlan 1 name Data
set vlan 1 port 8 tag 1
set vlan 2 name Voice
```

```
set vlan 2 port 8 tag 2
set igmp disable vlan Voice
set interface 1 ip 192.168.1.50 255.255.255.0
set security acl ip SpectraLink permit cos 7 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
set security acl ip SpectraLink permit 0.0.0.0
255.255.255.255
commit security acl SpectraLink
set security acl map SpectraLink vlan Voice in
set security acl map SpectraLink vlan Voice out
```

The following configuration file provides an example configuration to support SpectraLink 8000 Wireless Telephones using WPA2-PSK:

```
# Configuration nvgen'd at 2007-7-26 22:53:41
# Image 5.0.11.4.0
# Model 2360
# Last change occurred at 2007-7-26 22:53:34
set ip route default 192.168.1.1 1
set system name WSS2360
set system ip-address 192.168.1.50
set system countrycode US
set timezone EST -5 0
set service-profile Voice ssid-name Voice
set service-profile Voice auth-fallthru last-resort
set service-profile Voice rsn-ie enable
set service-profile Voice cipher-tkip disable
set service-profile Voice cipher-ccmp enable
set service-profile Voice psk-phrase enter-a-passphrase
set service-profile Voice auth-psk enable
set service-profile Voice auth-dot1x disable
set service-profile Voice attr vlan-name Voice
set enablepass password enable-password
set user admin password admin-password
set radio-profile default service-profile Voice
set radio-profile default dtim-interval 3
set radio-profile default auto-tune channel-config
disable
set radio-profile default active-scan disable
set radio-profile default qos-mode svp
set dap 1 serial-id stpw20kc3 model 2330
set dap 1 name WAP-2330-2
set dap 1 radio 1 channel 11 tx-power 10 mode enable
set dap 1 radio 2 channel 40 tx-power 10 mode enable
set port type ap 1 model 2330 poe enable
```

```
set ap 1 name WAP-2330-1
set ap 1 radio 1 tx-power 10 mode enable
set ap 1 radio 2 channel 44 tx-power 10 mode enable
set ip https server enable
set port poe 1 enable
set vlan 1 name Data
set vlan 1 port 8 tag 1
set vlan 2 name Voice
set vlan 2 port 8 tag 2
set igmp disable vlan Voice
set interface 1 ip 192.168.1.50 255.255.255.0
set security acl ip SpectraLink permit cos 7 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
set security acl ip SpectraLink permit 0.0.0.0
255.255.255.255
commit security acl SpectraLink
set security acl map SpectraLink vlan Voice in
set security acl map SpectraLink vlan Voice out
```